Bull. Aust. Math. Soc. **109** (2024), 138–151
doi:10.1017/S0004972723000448

A DYNAMICAL SYSTEM PROOF OF NIVEN'S THEOREM AND ITS EXTENSIONS

CHATCHAWAN PANRAKSA, DETCHAT SAMART ✉ and SONGPON SRIWONGSA

(Received 8 February 2023; accepted 13 April 2023; first published online 21 June 2023)

Abstract

Niven's theorem asserts that $\{\cos(r\pi) \mid r \in \mathbb{Q}\} \cap \mathbb{Q} = \{0, \pm 1, \pm 1/2\}$. In this paper, we use elementary techniques and results from arithmetic dynamics to obtain an algorithm for classifying all values in the set $\{\cos(r\pi) \mid r \in \mathbb{Q}\} \cap K$, where K is an arbitrary number field.

2020 *Mathematics subject classification*: primary 37C25; secondary 11C08, 11R04, 33B10.

Keywords and phrases: Niven's theorem, algebraic numbers, arithmetic dynamics.

1. Introduction

Finding exact values of trigonometric functions is a classical problem. For the sake of simplicity, we will mainly focus on the cosine. Analogous results for other trigonometric functions can be deduced using simple identities like

$$\sin(\theta) = \cos\left(\frac{\pi}{2} - \theta\right), \quad \tan^2(\theta) = \frac{1 - \cos(2\theta)}{1 + \cos(2\theta)}.$$

Common trigonometric values which are usually covered in introductory trigonometry lessons include

$$\cos(0) = 1, \quad \cos\left(\frac{\pi}{6}\right) = \frac{\sqrt{3}}{2}, \quad \cos\left(\frac{\pi}{4}\right) = \frac{\sqrt{2}}{2}, \quad \cos\left(\frac{\pi}{3}\right) = \frac{1}{2}, \quad \cos\left(\frac{\pi}{2}\right) = 0.$$

There are many other exact values of the cosine which are not as common, such as

$$\cos\left(\frac{\pi}{12}\right) = \frac{\sqrt{6} + \sqrt{2}}{4}, \quad \cos\left(\frac{\pi}{5}\right) = \frac{1 + \sqrt{5}}{4}.$$

The second author is supported by National Research Council of Thailand (NRCT) under the Research Grant for Mid-Career Scholar no. N41A640153. The third author acknowledges funding by the Office of the Permanent Secretary, Ministry of Higher Education, Science, Research and Innovation (OPS MHESI), Thailand Science Research and Innovation (TSRI) and King Mongkut's University of Technology Thonburi (Grant No. RGNS 64-096).

Observe that all of these values are expressible using only arithmetic operations and square roots, so they are algebraic numbers. In fact, by suitably applying de Moivre's formula, it can be seen that $\cos(r\pi)$ is an algebraic number for any $r \in \mathbb{Q}$ (see, for example, [7]). However, if r is an *irrational algebraic number*, then it follows from the Gelfond–Schneider theorem [12, Theorem 10.1] that $\cos(r\pi)$ is transcendental. It is therefore an interesting problem to explicitly determine values of $\cos(r\pi)$ when r is rational. Since algebraic number fields, that is, finite field extensions of $\mathbb{Q}$, constitute the field of algebraic numbers, this problem can also be rephrased as follows.

PROBLEM 1.1. Given a number field K, find all elements in K which are values of the cosine at a rational multiple of π.

By the Abel–Ruffini theorem, if K is a number field of degree higher than four, it might not be possible to write an element of K in a closed form. By 'explicitly determining' an algebraic number α, we generally refer to finding the minimal polynomial of α. It should be remarked that Problem 1.1 is neither new nor open; its complete solution, in some sense, has been known for some time now (see a remark after Theorem 1.4 below). A prime example is the following theorem, which corresponds to the case $K = \mathbb{Q}$.

THEOREM 1.2 (Niven's theorem, [12], Corollary 3.12). *If r and $\cos(r\pi)$ are both rational, then $\cos(r\pi) \in \{0, \pm 1, \pm 1/2\}$.*

Elementary proofs of Theorem 1.2 are given in [7, 14, 15]. The next result can be seen as an extension of Niven's theorem to quadratic number fields.

THEOREM 1.3. *Let $r \in \mathbb{Q}$. If $\cos(r\pi)$ is a quadratic irrationality, then*

$$\cos(r\pi) \in \left\{ \pm \frac{\sqrt{2}}{2}, \pm \frac{\sqrt{3}}{2}, \frac{\pm 1 \pm \sqrt{5}}{4} \right\}.$$

Using values of the cosine listed at the beginning of this section, one sees that the quadratic irrational values of $\cos(r\pi)$, with r rational, correspond to $r \in \{\pm 1/4, \pm 1/6, \pm 1/5, \pm 2/5\}$. Jahnel [7] proved Theorem 1.3 using standard tools from algebraic number theory such as prime ideal decomposition and general forms of quadratic integers. We refer the reader to recent work of the second-named author [17] for an alternative proof of this theorem which relies purely on basic notions in elementary number theory. For number fields of higher degree, we have the following general result, which is originally due to Lehmer ([8], see also [12, Theorem 3.9]).

THEOREM 1.4. *Let $m, n \in \mathbb{Z}$, with $n > 2$, be relatively prime. Then $\cos(2\pi m/n)$ is an algebraic number of degree $\varphi(n)/2$, where $\varphi(n)$ is Euler's totient function.*

With the help of this result, one can resolve Problem 1.1 for a number field K of degree $D > 1$ by finding all $n \in \mathbb{N}$ for which $\varphi(n) \mid 2D$ and determining all distinct values among $\cos(2\pi m/n)$, where $m \in \{1, 2, \ldots, n\}$ and $(m, n) = 1$, which belong to K. Since $\varphi(n) \geq \sqrt{n/2}$ for all $n \in \mathbb{N}$, there can be at most finitely many n for which we have $\varphi(n) \mid 2D$ for any fixed $D \in \mathbb{N}$.

https://doi.org/10.1017/S0004972723000448 Published online by Cambridge University Press

Proofs of the main results in [7, 14, 15, 17] make use of the double-angle formula

$$\cos(2\theta) = 2\cos^2(\theta) - 1. \tag{1.1}$$

If we define $F : \mathbb{R} \to \mathbb{R}$ by $F(x) = 2\cos(x)$, then it is obvious from (1.1) that $F(x)$ satisfies the functional equation $F(2x) = (F(x))^2 - 2$, from which one can deduce that, for any nonnegative integer k,

$$F(2^k x) = f^{(k)}(F(x)),$$

where $f(x) = x^2 - 2$ and $f^{(k)}$ denotes the k-fold composition of f with itself. By periodicity of the cosine, the set $\{F(2^k r\pi) \mid k \geq 0\}$ is finite for any $r \in \mathbb{Q}$. Niven's theorem can then be proven easily by iteratively applying $f(x)$ to a rational value of $F(r\pi)$ and using the fact that $F(x) \in [-2, 2]$ for any $x \in \mathbb{R}$. Observe that this argument has a dynamical flavour as it involves iteration of the rational map $f(x) = x^2 - 2$. Therefore, we have an intuitive conviction that these proofs can be rewritten in the language of dynamical systems. The main purpose of this article is to present a systematic approach to solving Problem 1.1 using ideas from arithmetic dynamics. Our first main result is the following theorem.

THEOREM 1.5. *Let K be a number field and let $C(K) := \{2\cos(r\pi) \mid r \in \mathbb{Q}\} \cap K$. Define $f : K \to K$ by $f(x) = x^2 - 2$. Then $C(K) = \mathrm{PrePer}(f, K)$, where $\mathrm{PrePer}(f, K)$ denotes the set of preperiodic points of f in K.*

Problem 1.1 then boils down to finding the preperiodic points of $f(x) = x^2 - 2$ over K. By Northcott's theorem [13], the set $\mathrm{PrePer}(f, K)$ is finite for any number field K. Although determining all elements of this set in general is not an easy task, there exists a procedure which allows us to compute them in a finite number of steps. More precisely, we shall prove the following result.

THEOREM 1.6. *Let K be a number field of degree D and let $\alpha \in K$ be a periodic point of $f(x) = x^2 - 2$ with minimal period n. Then $n \mid D$. In particular, $f^{(D)}(\alpha) = \alpha$.*

Choosing $K = \mathbb{Q}$ in Theorem 1.6, one sees that the rational periodic points of f must be its fixed points. In general, the periodic points of f which belong to some number field of degree D are exactly the zeros of irreducible factors of the polynomial $f^{(D)}(x) - x$ whose degrees do not exceed D. Since all preperiodic points can be obtained from the periodic points via the inverse mappings of f, we can systematically compute $\mathrm{PrePer}(f, K)$ using this result. Detailed computations over number fields of degree up to five will be illustrated in Section 4. We prove Theorems 1.5, 1.6 and some other related results in Section 3. In the next section, we review basic definitions and notions in arithmetic dynamics. Especially, we invoke some known results about dynamical properties of the map $f(x) = x^2 - 2$, which are crucial for the proof of Theorem 1.6.

https://doi.org/10.1017/S0004972723000448 Published online by Cambridge University Press

2. Arithmetic dynamics of the map $f(x) = x^2 - 2$

For any map g from a set S to itself and $k \in \mathbb{N}$, we define $g^{(k)}(x) := \underbrace{g(g(\cdots g}_{k \text{ times}}(x)))$. We say that a point $P \in S$ is *periodic* with respect to g if $g^{(n)}(P) = P$ for some $n \in \mathbb{N}$ and we call the smallest such n the *minimal period* for P. The point P is said to be *preperiodic* if $g^{(m)}(P)$ is periodic for some $m \in \mathbb{N}$, which is equivalent to saying that the *forward orbit* $O_g(P) := \{g^{(k)}(P) \mid k \geq 0\}$ is finite. The set of preperiodic points of g (in S) is denoted by $\mathrm{PrePer}(g, S)$.

If a field K does not have characteristic 2, then any quadratic polynomial $g(x) = Ax^2 + Bx + C \in K[x]$ with $A \neq 0$ can be transformed into $f_c(x) = x^2 + c$ by changing variables:

$$f_c(x) = \varphi^{-1} \circ g \circ \varphi(x), \quad \varphi(x) = \frac{2x - B}{2A}, \quad c = \frac{B}{2} - \frac{B^2}{4} + AC.$$

The study of an orbit of a rational function plays a central role in arithmetic dynamics. For example, given a number field K, the Morton–Silverman uniform boundedness conjecture [11] asks if there is an upper bound for the number of preperiodic points of $f(x) \in K[x]$ depending only on $[K : \mathbb{Q}]$ and $\deg f$. It is still open for the family of quadratic polynomials with $K = \mathbb{Q}$. For periods 1, 2 and 3 of $f_c(x) \in \mathbb{Q}[x]$, we can explicitly describe the relationship between the rational preperiodic points and the parameter c (see [21]). In addition, it is known that $f_c(x)$ has no rational periodic points of minimal periods 4, 5 and 6 (conditionally on a version of the Birch and Swinnerton-Dyer conjecture) (see [5, 10, 19]). For polynomials with integral coefficients, by using a simple divisibility argument, it can be shown that all preperiodic points have periods at most 2. For a number field K and $c \in O_K$, a result in [4] implies that the set of preperiodic points of $f_c(x)$ is uniformly bounded depending only on $D = [K : \mathbb{Q}]$ (see also [22]). However, it is still interesting to find an explicit bound for the number of preperiodic points of an integral quadratic polynomial. In this paper, we describe the preperiodic points of $f_{-2}(x) = x^2 - 2$ over K, where the base field K varies.

An important tool to study preperiodic points of a polynomial is its *dynatomic polynomial*. A dynatomic polynomial is a polynomial that encodes information about the orbits of a point under iteration of a polynomial map $f(x)$. Given a polynomial $f(x)$ and a positive integer n, the nth *dynatomic polynomial* of f, denoted by $\Phi_{n,f}(x)$, is the polynomial whose roots are the points that remain fixed under iteration of $f(x)$ for exactly n steps. These fixed points are also called the *formal n-periodic points*, and are solutions of the equation $f^{(n)}(x) = x$. As an analogue of cyclotomic polynomials, the nth dynatomic polynomial can be computed using the formula

$$\Phi_{n,f}(x) = \prod_{d|n} (f^{(d)}(x) - x)^{\mu(n/d)},$$

https://doi.org/10.1017/S0004972723000448 Published online by Cambridge University Press

where μ is the Möbius function defined by $\mu(1) = 1$ and

$$\mu(p_1^{i_1} p_2^{i_2} \cdots p_k^{i_k}) = \begin{cases} (-1)^k & \text{if } i_j = 1 \text{ for all } j \in \{1, 2, \ldots, k\}, \\ 0 & \text{if } i_j \geq 2 \text{ for some } j \in \{1, 2, \ldots, k\}. \end{cases}$$

For example, the first few dynatomic polynomials of $f_c(x)$ are

$$\begin{aligned} \Phi_{1,f_c}(x) &= x^2 - x + c, \\ \Phi_{2,f_c}(x) &= x^2 + x + (c+1), \\ \Phi_{3,f_c}(x) &= x^6 + x^5 + (3c+1)x^4 + (2c+1)x^3 + (3c^2+3c+1)x^2 \\ &\quad + (c^2+2c+1)x + (c^3+2c^2+c+1). \end{aligned}$$

The dynatomic polynomials are important in the study of arithmetic dynamics, in particular in the study of the arithmetic and geometric properties of the orbits of points under iteration of polynomial maps. For more details of the dynatomic polynomials, see [3, 9, 18].

Vivaldi and Hatjispyros [20, Section 5.2] explicitly described the nth dynatomic polynomial of $f(x) = x^2 - 2$.

THEOREM 2.1. *Let $f(x) = x^2 - 2$ and define $\Psi_m(x + x^{-1}) = \Phi_m(x)x^{-\varphi(m)/2}$, where $\Phi_m(x)$ is the cyclotomic polynomial of order m. Then*

$$\Phi_{n,f}(x) = \prod_{d|n} \Bigg(\prod_{d_1|2^d-1} \Psi_{d_1}(x) \prod_{d_2|2^d+1} \Psi_{d_2}(x) \Bigg)^{\mu(n/d)}.$$

REMARK 2.2. It is known that $\Psi_1^2(x) = x - 2, \Psi_2^2(x) = x + 2$ and, for $m > 2$, $\Psi_m(x)$ is an irreducible polynomial with integer coefficients [12, Lemma 3.8]. In fact, it can be seen from a proof of Theorem 1.4 that $\Psi_m(x)$ is the minimal polynomial of the algebraic integer $2\cos(2\pi/m)$, so $\deg \Psi_m = \varphi(m)/2$.

3. Proofs of the main results

PROOF OF THEOREM 1.5. Let $\alpha = m\pi/n$, where $m, n \in \mathbb{Z}$ with $n > 0$, and let

$$X_n := \{2\cos(j\pi/n) \mid j \in \mathbb{Z}\}.$$

Suppose that $\gamma := 2\cos(\alpha) \in K$. Then we have

$$f(\gamma) = 4\cos^2(\alpha) - 2 = 2\cos(2\alpha) \in X_n.$$

It follows that $O_f(\gamma) = \{2\cos(2^k\alpha) \mid k \geq 0\} \subseteq X_n$. By the periodicity of the cosine, the set X_n is finite, so $O_f(\gamma)$ must also be finite. Hence, $\gamma \in \mathrm{PrePer}(f, K)$.

Conversely, let $\delta \in \mathrm{PrePer}(f, K)$. Then there exists $k \in \mathbb{N}$ for which $\beta := f^{(k)}(\delta)$ is periodic. We first show that $|\delta| \leq 2$. Assume to the contrary that $|\delta| > 2$. Then it is easy to see that $f^{(j)}(\delta) > 2$ for all $j \geq 1$. Moreover, we have

$$f^{(j+1)}(\delta) - f^{(j)}(\delta) = (f^{(j)}(\delta) - 2)(f^{(j)}(\delta) + 1) > 0,$$

https://doi.org/10.1017/S0004972723000448 Published online by Cambridge University Press

so the sequence $\{f^{(j)}(\delta)\}_{j=1}^{\infty}$ is strictly increasing. Hence, $f^{(j)}(\delta)$ is not periodic for any $j \in \mathbb{N}$, which is a contradiction. Therefore, we may conclude by continuity of the cosine that $\delta = 2\cos(r\pi)$ for some $r \in \mathbb{R}$. Since β is periodic, there exists $l \in \mathbb{N}$ such that

$$2\cos(2^k r\pi) = f^{(k)}(\delta) = \beta = f^{(l)}(\beta) = f^{(k+l)}(\delta) = 2\cos(2^{k+l} r\pi).$$

Thus, $2^k r\pi = \pm 2^{k+l} r\pi + 2t\pi$ for some $t \in \mathbb{Z}$. It is clear from this equation that r is rational, so $\delta \in C(K)$ as desired. □

REMARK 3.1. In fact, Theorem 1.5 holds for any *Chebyshev polynomial* P_n defined by

$$P_1(x) = x, \quad P_2(x) = x^2 - 2 \quad \text{and} \quad P_{m+1}(x) = xP_m(x) - P_{m-1}(x) \quad \text{for } m \geq 2.$$

A proof of this more general result can be found in [6, Proposition 2.2.2]. Since our proof is quite simple and should be accessible to a more general audience, we decided to include it here rather than solely referring to the result above.

It is a well-known fact that if r is rational, then $2\cos(r\pi)$ is an algebraic integer. Proofs of this result using the theory of algebraic numbers can be found in [12, Theorem 3.9] and [7]. However, we shall apply Theorem 1.5 to prove this fact, without resorting to any advanced machinery in algebraic number theory.

COROLLARY 3.2. *Let K be a number field. Then $C(K) \subseteq O_K$, where O_K denotes the ring of algebraic integers of K.*

PROOF. Let $\gamma \in C(K)$. Then by Theorem 1.5, there exists $m \in \mathbb{N}$ such that $f^{(m)}(\gamma)$ is a periodic point, where $f(x) = x^2 - 2$. Hence, there exists $l \in \mathbb{N}$ such that

$$f^{(l+m)}(\gamma) = f^{(l)}(f^{(m)}(\gamma)) = f^{(m)}(\gamma).$$

Let $h(x) = f^{(l+m)}(x) - f^{(m)}(x)$. Then it is obvious that $h(x) \in \mathbb{Z}[x]$ is monic and annihilates γ. Therefore, $\gamma \in O_K$. □

Using Theorems 1.4 and 1.5, one can easily obtain an explicit upper bound for the order of $\mathrm{PrePer}(f, K)$ in terms of $[K : \mathbb{Q}]$, in line with Northcott's theorem.

COROLLARY 3.3. *Let K be a number field of degree D and $f(x) = x^2 - 2$. Then,*

$$|\mathrm{PrePer}(f, K)| \leq \sum_{n=1}^{8D^2} \varphi(n).$$

PROOF. By Theorems 1.4 and 1.5,

$$\mathrm{PrePer}(f, K) \subseteq \left\{ 2\cos\left(2\pi \frac{m}{n}\right) : n \in \mathbb{N}, \varphi(n) \mid 2D, 1 \leq m < n, (m, n) = 1 \right\}.$$

If $\varphi(n) \mid 2D$, then by a trivial lower bound for $\varphi(n)$, we have $\sqrt{n/2} \leq \varphi(n) \leq 2D$, implying $n \leq 8D^2$. Hence, the cardinality of the set on the right-hand side is at most $\sum_{n=1}^{8D^2} \varphi(n)$. □

https://doi.org/10.1017/S0004972723000448 Published online by Cambridge University Press

REMARK 3.4. The summation in Corollary 3.3 can be written as a value of the *totient summatory function* $\Phi(m) := \sum_{n=1}^{m} \varphi(n)$, which satisfies an asymptotic formula

$$\Phi(m) \sim \frac{3m^2}{\pi^2} + O(m \log m).$$

One can modify a proof of this formula to obtain a simpler upper bound for $|\mathrm{PrePer}(f, K)|$. Note, however, that this bound is very far from optimal. One way to improve it is to use a stronger lower bound for $\varphi(n)$. For instance, it is known from [1, Theorem 8.8.7] that for $n > 2$,

$$\varphi(n) > \frac{n}{e^{\gamma} \log\log n + \dfrac{3}{\log\log n}},$$

where γ is Euler's constant.

To prove Theorem 1.6, we need the following auxiliary results about divisors of $2^l \pm 1$, where l is a prime power. Recall that for a prime p and a nonzero integer s, the *p-adic valuation of s*, denoted by $v_p(s)$, is the exponent of the highest power of p that divides s.

LEMMA 3.5. *Let $k \in \mathbb{N}$.*

(i) *If $k > 1$ and q is a prime divisor of $2^{2^k} + 1$, then $q = 2^{k+2}m + 1$ for some $m \in \mathbb{N}$.*
(ii) *For any odd prime p, if q is a prime divisor of $2^{p^k} - 1$ (respectively $2^{p^k} + 1$) and $q \nmid 2^{p^{k-1}} - 1$ (respectively $q \nmid 2^{p^{k-1}} + 1$), then $q = 2p^k m + 1$ for some $m \in \mathbb{N}$.*
(iii) *For any odd prime p,*

$$v_3(2^{p^k} + 1) = \begin{cases} k+1 & \text{if } p = 3, \\ 1 & \text{if } p > 3, \end{cases} \tag{3.1}$$

$$v_3(2^{p^k} - 1) = 0. \tag{3.2}$$

PROOF. (i) This assertion is known as the Euler–Lucas theorem [4, Theorem 1.3.5], which gives an explicit form of the prime divisors of Fermat numbers.

(ii) Recall that for a positive integer n and an integer a which is relatively prime to n, the *order of a modulo n*, denoted by $\mathrm{ord}_n a$, is the smallest positive integer r such that

$$a^r \equiv 1 \pmod{n}.$$

Indeed, for any $s \in \mathbb{N}$, if $a^s \equiv 1 \pmod{n}$, then $\mathrm{ord}_n a \mid s$. Let p be an odd prime and let q be a prime divisor of $2^{p^k} - 1$, where $q \nmid 2^{p^{k-1}} - 1$. Then it follows immediately that $\mathrm{ord}_q 2 = p^k$. Since q is odd, $2^{q-1} \equiv 1 \pmod{q}$ by Fermat's little theorem, implying $p^k \mid q - 1$. Moreover, since $2 \mid q - 1$ and $q > 1$, we have $q = 2p^k m + 1$ for some integer $m \geq 1$, as desired.

https://doi.org/10.1017/S0004972723000448 Published online by Cambridge University Press

Next, assume that $q \mid 2^{p^k}+1$, but $q \nmid 2^{p^{k-1}}+1$. Obviously, $3 \mid 2^l+1$ for every $l \in \mathbb{N}$, so $q > 3$. Observe that

$$2^{2p^k} = (2^{p^k})^2 \equiv (-1)^2 = 1 \pmod{q},$$

so $\operatorname{ord}_q 2 \mid 2p^k$. Since $q \neq 3$, we have $\operatorname{ord}_q 2 \neq 2$. Moreover, since $2^{p^{k-1}} \not\equiv \pm 1 \pmod{q}$, we have $2^{2p^{k-1}} \not\equiv 1 \pmod{q}$. Therefore, we can conclude that $\operatorname{ord}_q 2 = 2p^k$. Again, by Fermat's little theorem, we can write $q = 2p^k m + 1$ for some $m \in \mathbb{N}$.

(iii) Applying the lifting-the-exponent lemma [2, Theorem 6.2], one sees immediately that (3.1) holds. In addition, since $3 \mid 2^{p^k}+1$, we have $2^{p^k} - 1 \equiv -2 \bmod 3$, which yields (3.2). □

LEMMA 3.6. *Let $t = p^k$, where p is prime and $k \in \mathbb{N}$. Then the degree of each irreducible factor of $\Phi_{t,f}(x)$ over $\mathbb{Q}$ is a multiple of t.*

PROOF. We divide the proof into three cases, according to the value of p.

Case $p = 2$. From Theorem 2.1,

$$\begin{aligned}\Phi_{t,f}(x) &= \prod_{r=0}^{k}\Bigg(\prod_{d_1 \mid 2^{2^r}-1}\Psi_{d_1}(x)\prod_{d_2 \mid 2^{2^r}+1}\Psi_{d_2}(x)\Bigg)^{\mu(2^{k-r})}\\ &= \prod_{d_1 \mid 2^{2^k}-1}\Psi_{d_1}(x)\prod_{d_2 \mid 2^{2^k}+1}\Psi_{d_2}(x)\prod_{d_1 \mid 2^{2^{k-1}}-1}\Psi_{d_1}(x)^{-1}\prod_{d_2 \mid 2^{2^{k-1}}+1}\Psi_{d_2}(x)^{-1}\\ &= \prod_{\substack{c_1 \mid 2^{2^{k-1}}-1\\ c_2 \mid 2^{2^{k-1}}+1\\ c_1,c_2>1}}\Psi_{c_1c_2}(x)\prod_{\substack{d_2 \mid 2^{2^k}+1\\ d_2>1}}\Psi_{d_2}(x),\end{aligned}$$

where we have used the trivial factorisation $2^{2^k} - 1 = (2^{2^{k-1}} - 1)(2^{2^{k-1}} + 1)$ to deduce the last equality. If $k = 1$, then $\Phi_{t,f}(x) = \Psi_5(x)$, which is a quadratic polynomial. If $k = 2$, then $\Phi_{t,f}(x) = \Psi_{15}(x)\Psi_{17}(x)$, where $\deg \Psi_{15} = 4$ and $\deg \Psi_{17} = 8$. It remains to consider $k > 2$. Let $c_1, c_2 > 1$ be divisors of $2^{2^{k-1}} - 1$ and $2^{2^{k-1}} + 1$, respectively. Since $2^{2^{k-1}} - 1$ and $2^{2^{k-1}} + 1$ are coprime, so are c_1 and c_2. Let q be a prime divisor of c_2. Then there exist $l, s \in \mathbb{N}$ such that $c_2 = lq^s$ and $\gcd(l, q) = 1$. Moreover, from Lemma 3.5(i), $q = 2^{k+1}m + 1$ for some $m \in \mathbb{N}$. By the remark under Theorem 2.1 and multiplicativity of φ, we have

$$\deg \Psi_{c_1c_2} = \frac{\varphi(c_1c_2)}{2} = \frac{\varphi(c_1)\varphi(c_2)}{2} = \frac{\varphi(c_1)\varphi(l)q^{s-1}(q-1)}{2} = \varphi(c_1)\varphi(l)q^{s-1}2^k m,$$

so $t = 2^k \mid \deg \Psi_{c_1c_2}$. It can be shown using the same argument that $2^k \mid \deg \Psi_{d_2}$ for any divisor $d_2 > 1$ of $2^{2^k} + 1$.

https://doi.org/10.1017/S0004972723000448 Published online by Cambridge University Press

Case $p = 3$. By Theorem 2.1,

$$\Phi_{t,f}(x) = \prod_{\substack{d_1 \mid 2^{3^k}-1 \\ d_1 \nmid 2^{3^{k-1}}-1}} \Psi_{d_1}(x) \prod_{\substack{d_2 \mid 2^{3^k}+1 \\ d_2 \nmid 2^{3^{k-1}}+1}} \Psi_{d_2}(x).$$

Let d_1 be a positive divisor of $2^{3^k} - 1$, where $d_1 \nmid 2^{3^{k-1}} - 1$. Since

$$2^{3^k} - 1 = (2^{3^{k-1}} - 1)((2^{3^{k-1}})^2 + 2^{3^{k-1}} + 1),$$

and by (3.2),

$$\gcd(2^{3^{k-1}} - 1, (2^{3^{k-1}})^2 + 2^{3^{k-1}} + 1) = \gcd(2^{3^{k-1}} - 1, 2^{3^{k-1}} + 2) = \gcd(2^{3^{k-1}} - 1, 3) = 1,$$

there exists a prime divisor q of d_1 such that $q \nmid 2^{3^{k-1}} - 1$. Let $s = v_q(d_1)$ and $l = d_1/q^s$. By Lemma 3.5(ii), $q = 2(3^k m) + 1$ for some $m \in \mathbb{N}$, whence

$$\deg \Psi_{d_1} = \frac{\varphi(d_1)}{2} = \frac{\varphi(l)q^{s-1}(q-1)}{2} = \varphi(l)q^{s-1}3^k m.$$

Now let d_2 be a positive divisor of $2^{3^k} + 1$, where $d_2 \nmid 2^{3^{k-1}} + 1$. Observe that

$$2^{3^k} + 1 = (2^{3^{k-1}} + 1)((2^{3^{k-1}})^2 - 2^{3^{k-1}} + 1),$$

where

$$\gcd(2^{3^{k-1}} + 1, (2^{3^{k-1}})^2 - 2^{3^{k-1}} + 1) = \gcd(2^{3^{k-1}} + 1, 2^{3^{k-1}} - 2) = \gcd(2^{3^{k-1}} + 1, 3) = 3.$$

If d_2 is a power of 3, then $d_2 = 3^{k+1}$ from (3.1), in which case

$$\deg \Psi_{d_2} = \frac{\varphi(d_2)}{2} = 3^k.$$

Otherwise, d_2 has a prime divisor $q > 3$ such that $q \nmid 2^{3^{k-1}} + 1$, so we can again employ Lemma 3.5(ii) to deduce that $3^k \mid \deg \Psi_{d_2}$.

Case $p > 3$. By Theorem 2.1,

$$\Phi_{t,f}(x) = \prod_{\substack{d_1 \mid 2^{p^k}-1 \\ d_1 \nmid 2^{p^{k-1}}-1}} \Psi_{d_1}(x) \prod_{\substack{d_2 \mid 2^{p^k}+1 \\ d_2 \nmid 2^{p^{k-1}}+1}} \Psi_{d_2}(x).$$

Simple calculations yield

$$2^{p^k} - 1 = (2^{p^{k-1}} - 1)m_1, \quad 2^{p^k} + 1 = (2^{p^{k-1}} + 1)m_2,$$

https://doi.org/10.1017/S0004972723000448 Published online by Cambridge University Press

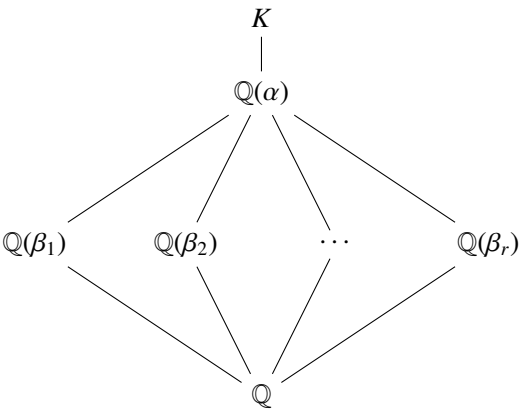


FIGURE 1. Diagram for the proof of Theorem 1.6.

where $m_1 > 1$, $m_2 > 1$ and $\gcd(2^{p^{k-1}} - 1, m_1) = \gcd(2^{p^{k-1}} + 1, m_2) = 1$. Hence, for any d_1 and d_2 in the product above, there exist prime divisors q_1 and q_2 of d_1 and d_2 such that $q_1 \nmid 2^{p^{k-1}} - 1$ and $q_2 \nmid 2^{p^{k-1}} + 1$. Then, with the aid of Lemma 3.5(ii), it can be shown using arguments in the same vein as those in the previous cases that $p^k \mid \deg \Psi_{d_1}$ and $p^k \mid \deg \Psi_{d_2}$. □

PROOF OF THEOREM 1.6. The case $n = 1$ is trivial, so we may assume that $n > 1$. By the fundamental theorem of arithmetic, we can write n as $n = p_1^{a_1} \cdots p_r^{a_r}$, where $r, a_1, \ldots, a_r \in \mathbb{N}$ and $p_1, \ldots, p_r$ are distinct primes. For $1 \le i \le r$, let $n_i = n/p_i^{a_i}$ and $\beta_i = f^{(n_i)}(\alpha) \in \mathbb{Q}(\alpha) \subseteq K$. Then β_i is a periodic point of f with minimal period $p_i^{a_i}$. Recall that the periodic points of f with minimal period l in $\overline{\mathbb{Q}}$ are zeros of $\Phi_{l,f}(x)$. Hence, β_i must be a root of an irreducible factor $\tau_i(x)$ of $\Phi_{p_i^{a_i},f}(x)$. By Lemma 3.6, for $1 \le i \le r$,

$$p_i^{a_i} \mid \deg \tau_i = [\mathbb{Q}(\beta_i) : \mathbb{Q}].$$

Moreover, since $[\mathbb{Q}(\beta_i) : \mathbb{Q}] \mid [K : \mathbb{Q}]$ (see Figure 1), it follows that $n = \operatorname{lcm}(p_1^{a_1}, \ldots, p_r^{a_r}) \mid [K : \mathbb{Q}]$, as desired. □

4. Examples in number fields of low degree

In this section, we apply our results to classify all values of the cosine at a rational multiple of π which belong to a number field K of degree D with $1 \le D \le 5$. We start by factoring the polynomial $f^{(D)}(x) - x$. By Theorem 1.6, the periodic points of f in K can be obtained from zeros of irreducible factors of $f^{(D)}(x) - x$ which have degree at most D. All the preperiodic points of f in K can then be computed by taking preimages of these values under f, which can be done in a finite number of steps.

https://doi.org/10.1017/S0004972723000448 Published online by Cambridge University Press

EXAMPLE 4.1. For $D = 1$, we have $K = \mathbb{Q}$ and the periodic points must be fixed points of f. Since $f(x) - x = x^2 - x - 2 = (x + 1)(x - 2)$, we have the following two digraphs representing all rational preperiodic points of f:

$$0 \longrightarrow -2 \longrightarrow 2 \circlearrowright \qquad\qquad 1 \longrightarrow -1 \circlearrowright$$

Here, $a \to b$ means $f(a) = b$. In other words, we have $\mathrm{PrePer}(f, \mathbb{Q}) = \{0, \pm 1, \pm 2\}$, which is equivalent to Niven's theorem.

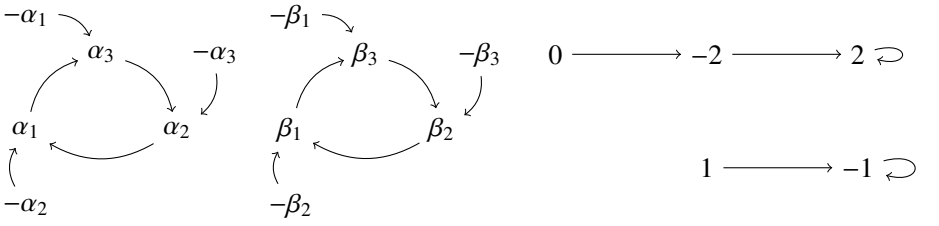
EXAMPLE 4.2. For $D = 2$, K is a quadratic number field; that is, $K = \mathbb{Q}(\sqrt{m})$ for some square-free integer m and $f^{(2)}(x) - x = x^4 - 4x^2 - x + 2 = (x - 2)(x + 1)(x^2 + x - 1)$. Hence, the preperiodic points of f in K can be seen from the following three digraphs, thereby proving Theorem 1.3:

$$\pm\sqrt{2} \longrightarrow 0 \longrightarrow -2 \longrightarrow 2 \circlearrowright$$

$$\pm\sqrt{3} \longrightarrow 1 \longrightarrow -1 \circlearrowright$$

$$\frac{1+\sqrt{5}}{2} \longrightarrow \frac{-1+\sqrt{5}}{2} \circlearrowright \frac{-1-\sqrt{5}}{2} \longleftarrow \frac{1-\sqrt{5}}{2}$$

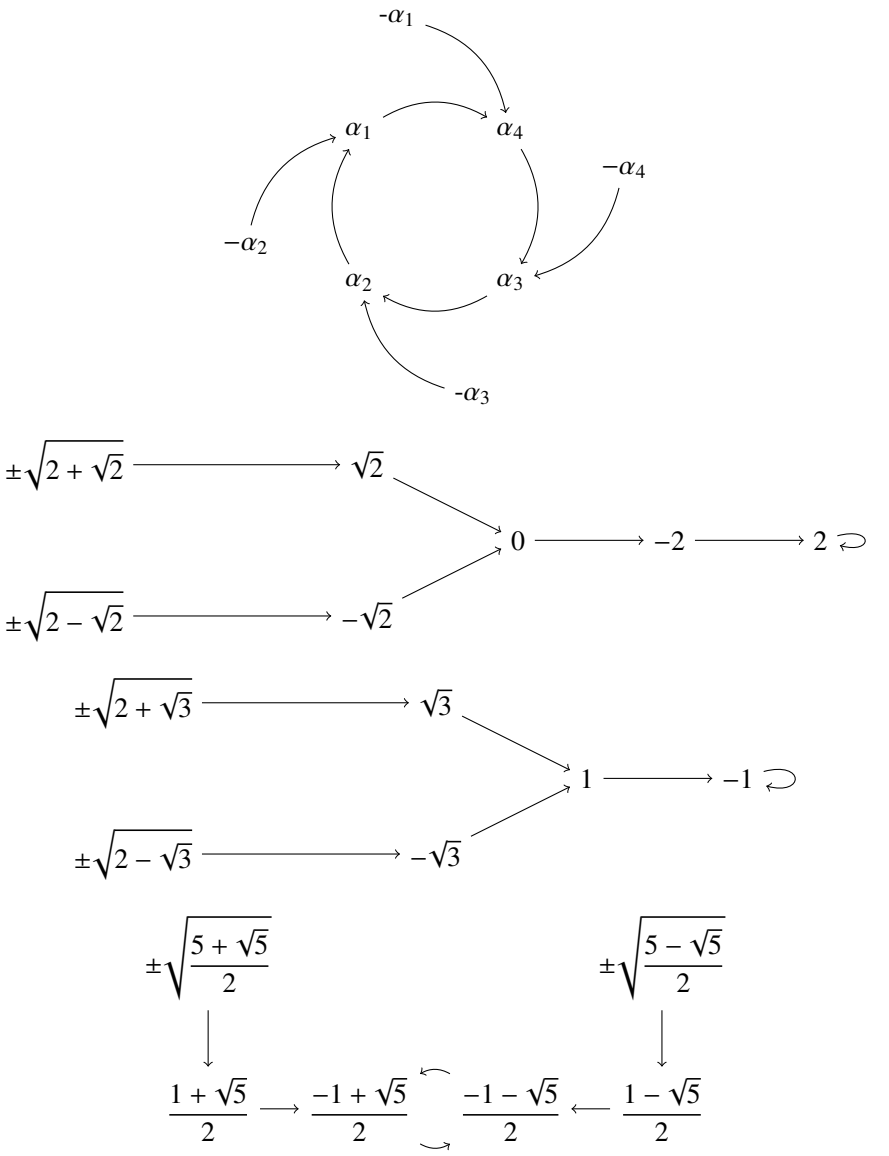
EXAMPLE 4.3. For $D = 3$, $f^{(3)}(x) - x = (x - 2)(x + 1)(x^3 - 3x + 1)(x^3 + x^2 - 2x - 1)$. Suppose that $\alpha_1 < \alpha_2 < \alpha_3$ and $\beta_1 < \beta_2 < \beta_3$ are all roots of the third and the fourth factors, respectively. The following four digraphs represent all preperiodic points in cubic fields:



Therefore, $\{\pm\alpha_1, \pm\alpha_2, \pm\alpha_3, \pm\beta_1, \pm\beta_2, \pm\beta_3\}$ is the set of all cubic irrational values of $2\cos(r\pi)$, where $r \in \mathbb{Q}$.

EXAMPLE 4.4. For $D = 4$, we have $f^{(4)}(x) - x = (x - 2)(x + 1)(x^2 + x - 1)(x^4 - x^3 - 4x^2 + 4x + 1)(x^8 + x^7 - 7x^6 - 6x^5 + 15x^4 + 10x^3 - 10x^2 - 4x + 1)$. Let $\alpha_1 < \alpha_2 < \alpha_3 < \alpha_4$ be the roots of the quartic factor of $f^{(4)}(x) - x$. Then we have the following four digraphs:

https://doi.org/10.1017/S0004972723000448 Published online by Cambridge University Press



Therefore, the set of all quartic irrational values of $2\cos(r\pi)$, for $r \in \mathbb{Q}$, is

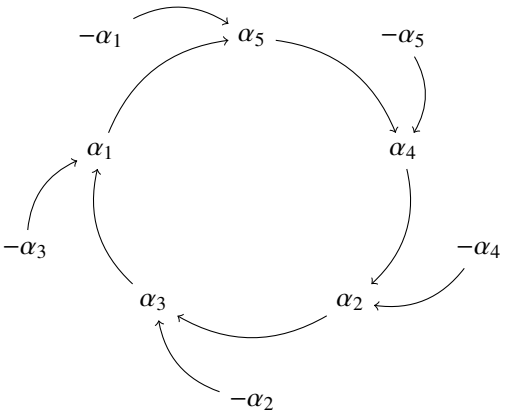
$$\left\{ \pm\alpha_1, \pm\alpha_2, \pm\alpha_3, \pm\alpha_4, \pm\sqrt{2 \pm \sqrt{2}}, \pm\sqrt{2 \pm \sqrt{3}}, \pm\sqrt{\frac{5 \pm \sqrt{5}}{2}} \right\}.$$

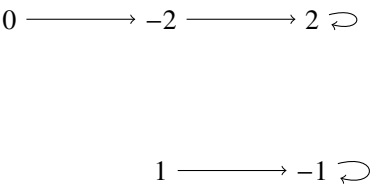
EXAMPLE 4.5. For $D = 5$, we can factorise

$$f^{(5)}(x) - x = (x-2)(x+1)(x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1) \cdot g(x) \cdot h(x),$$

https://doi.org/10.1017/S0004972723000448 Published online by Cambridge University Press

where $g(x)$ and $h(x)$ are irreducible polynomials with $\deg g = 10$ and $\deg h = 15$. Let $\alpha_1 < \alpha_2 < \alpha_3 < \alpha_4 < \alpha_5$ be the roots of the quintic factor of $f^{(5)}(x) - x$. Then we have the following digraphs:





Therefore, $\{\pm\alpha_1, \pm\alpha_2, \pm\alpha_3, \pm\alpha_4, \pm\alpha_5\}$ is the set of all quintic irrational values of $2\cos(r\pi)$, where $r \in \mathbb{Q}$.

5. Closing remarks

The dynamical properties of the map $f_c(x) = x^2 + c$ have been studied extensively over the past few decades, yet many related problems still remain open. For $c = -2$, this map turns out to be closely related to a classical result in number theory, namely Niven's theorem and its extensions. This relation can be seen directly from Theorem 1.5. We can then apply Theorem 1.6 to systematically classify all preperiodic points of $f_{-2}(x)$ in any number field K. It should be remarked that our proof of Theorem 1.6 relies crucially on the known result [20] about factorisation of the dynatomic polynomials associated to $f_{-2}(x)$, so it should not be expected that this theorem holds for $f_c(x)$ in general. As a concrete example, consider $f_{-1}(x) = x^2 - 1$. It is clear that 0 is a periodic point of $f_{-1}(x)$ with minimal period 2, so 0 is not a fixed point of $f_{-1}(x)$. To determine all values of $c \in \mathbb{Q}$ for which $f_c(x)$ satisfies the property in Theorem 1.6, one might start from those in [16, Figure 1] which correspond to digraphs containing no cycles of length greater than 1; that is, $c \in \{1, 1/4, 0, -2, -3/4, -10/9\}$. For each of these values, it is also an interesting problem to interpret the preperiodic points of $f_c(x)$ as special values of some function.

References

[1] E. Bach and J. Shallit, *Algorithmic Number Theory, Volume 1: Efficient Algorithms*, Foundations of Computing Series (MIT Press, Cambridge, MA, 1996).
[2] M. Billal and S. Riasat, *Integer Sequences: Divisibility, Lucas and Lehmer Sequences* (Springer, Singapore, 2021).
[3] T. Bousch, *Sur quelques problèmes de dynamique holomorphe*, PhD Thesis, Paris 11, 1992.

https://doi.org/10.1017/S0004972723000448 Published online by Cambridge University Press

[4] J. K. Canci and L. Paladino, 'Preperiodic points for rational functions defined over a global field in terms of good reduction', *Proc. Amer. Math. Soc.* **144**(12) (2016), 5141–5158.
[5] E. V. Flynn, B. Poonen and E. F. Schaefer, 'Cycles of quadratic polynomials and rational points on a genus-2 curve', *Duke Math. J.* **90**(3) (1997), 435–463.
[6] S.-I. Ih and T. J. Tucker, 'A finiteness property for preperiodic points of Chebyshev polynomials', *Int. J. Number Theory* **6**(5) (2010), 1011–1025.
[7] J. Jahnel, 'When is the (co)sine of a rational angle equal to a rational number?', Preprint, 2010, arXiv:1006.2938.
[8] D. H. Lehmer, 'Questions, discussions, and notes: a note on trigonometric algebraic numbers', *Amer. Math. Monthly* **40**(3) (1933), 165–166.
[9] P. Morton, 'On certain algebraic curves related to polynomial maps', *Compos. Math.* **103**(3) (1996), 319–350.
[10] P. Morton, 'Arithmetic properties of periodic points of quadratic maps. II', *Acta Arith.* **87**(2) (1998), 89–102.
[11] P. Morton and J. H. Silverman, 'Rational periodic points of rational functions', *Int. Math. Res. Not. IMRN* **1994**(2) (1994), 97–110.
[12] I. Niven, *Irrational Numbers*, The Carus Mathematical Monographs, 11 (Mathematical Association of America; distributed by John Wiley, New York, 1956).
[13] D. G. Northcott, 'Periodic points on an algebraic variety', *Ann. of Math. (2)* **51** (1950), 167–177.
[14] B. Paolillo and G. Vincenzi, 'An elementary proof of Niven's theorem via the tangent function', *Internat. J. Math. Ed. Sci. Tech.* **52**(6) (2021), 959–964.
[15] B. Paolillo and G. Vincenzi, 'On the rational values of trigonometric functions of angles that are rational in degrees', *Math. Mag.* **94**(2) (2021), 132–134.
[16] B. Poonen, 'The classification of rational preperiodic points of quadratic polynomials over Q: a refined conjecture', *Math. Z.* **228**(1) (1998), 11–29.
[17] D. Samart, 'On an extension of Niven's theorem', *Internat. J. Math. Ed. Sci. Tech.*, to appear. Published online (1 August 2022).
[18] J. H. Silverman, *The Arithmetic of Dynamical Systems*, Graduate Texts in Mathematics, 241 (Springer, New York, 2007).
[19] M. Stoll, 'Rational 6-cycles under iteration of quadratic polynomials', *LMS J. Comput. Math.* **11** (2008), 367–380.
[20] F. Vivaldi and S. Hatjispyros, 'Galois theory of periodic orbits of rational maps', *Nonlinearity* **5**(4) (1992), 961–978.
[21] R. Walde and P. Russo, 'Rational periodic points of the quadratic function $Q_c(x) = x^2 + c$', *Amer. Math. Monthly* **101**(4), 318–331.
[22] R. Zhang, 'The *abcd* conjecture, uniform boundedness, and dynamical systems', Preprint, 2022, arXiv:2206.09725.

CHATCHAWAN PANRAKSA, Applied Mathematics Program,
Mahidol University International College, Nakhon Pathom 73170, Thailand
e-mail: chatchawan.pan@mahidol.edu

DETCHAT SAMART, Department of Mathematics,
Faculty of Science, Burapha University, Chonburi 20131, Thailand
e-mail: petesamart@gmail.com

SONGPON SRIWONGSA, Department of Mathematics, Faculty of Science,
King Mongkut's University of Technology Thonburi, Bangkok 10140, Thailand
e-mail: songpon.sri@kmutt.ac.th

https://doi.org/10.1017/S0004972723000448 Published online by Cambridge University Press